

(11)Publication number : 2002-304805  
(43)Date of publication of application : 18.10.2002

(21)Application number : **2001-110541** (71)Applicant : **SONY CORP**  
(22)Date of filing : **09.04.2001** (72)Inventor : **ISHIZAKA TOSHIYA**  
**YAMADA MAKOTO**  
**ISHIGURO RYUJI**

[Date of request for examination]	21.02.2003
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	

**This Page Blank (uspto)**

**This Page Blank (uspto)**

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

**This Page Blank (uspto)**

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2002-304805  
(P2002-304805A)

(43)公開日 平成14年10月18日(2002.10.18)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	キーワード(参考)
G 1 1 B 20/10		C 1 1 B 20/10	H 5 B 0 1 7
G 0 6 F 12/00	5 1 1	C 0 6 F 12/00	5 1 1 C 5 B 0 8 2
	5 3 7		5 3 7 M 5 C 0 5 3
12/14	3 2 0	12/14	3 2 0 B 5 D 0 4 4
G 1 1 B 20/12		C 1 1 B 20/12	5 D 1 1 0
審査請求 未請求 請求項の数20 O L (全 19 頁) 最終頁に続く			

(21)出願番号 特願2001-110541(P2001-110541)

(22)出願日 平成13年4月9日(2001.4.9)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 石坂 敏弥

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 山田 誠

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74)代理人 100082762

弁理士 杉浦 正知

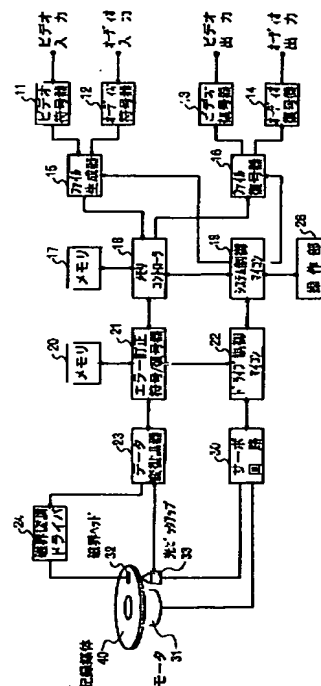
最終頁に続く

(54)【発明の名称】 無体財産権を保護する情報を記録する記録装置、記録方法および記録媒体

(57)【要約】

【課題】 本発明は、記録媒体上のデータに成立する無体財産権を保護する機能を備える記録装置、記録方法および記録媒体に関する。

【解決手段】 本発明の記録装置は、特殊なハードウェアを用いずに動画等を同期して再生するためのソフトウェアにより取り扱うことができるファイル構造を持つように、データのデータ構造を変換する変換手段15、18、19と、データを記録媒体に記録する記録手段23、24、32、33とを備え、ファイル構造は、実データである第1データ単位と、複数の第1データ単位の集合としての第2データ単位と、複数の第1データ単位間の関係と第1データ単位の実データの属性とを管理する管理情報を記述するためのデータ部分とを有し、データ部分に、データの無体財産権を保護するための保護情報を収容することで構成する。



【特許請求の範囲】

【請求項1】 データを書き換え可能な記録媒体に記録する記録装置において、

特殊なハードウェアを用いずに動画等を同期して再生するためのコンピュータソフトウェアにより取り扱うことができるファイル構造を持つように、前記データのデータ構造を変換する変換手段と、

前記ファイル構造に変換されたデータを前記記録媒体に記録する記録手段とを備え、

前記ファイル構造は、実データである第1データ単位と、複数の前記第1データ単位の集合としての第2データ単位と、複数の前記第1データ単位間の関係と第1データ単位の実データに関する属性とを管理する管理情報を記述するためのデータ部分とを有し、

前記データ部分に、前記第1データ単位に成立する無体財産権を保護するための保護情報を収容することを特徴とする記録装置。

【請求項2】 前記保護情報を、前記データ部分に収容する代わりに独立なファイルに収容し、前記データ部分には前記ファイルを指定する指定情報を収容することを特徴とする請求項1に記載の記録装置。

【請求項3】 前記実データは、所定の暗号方法で暗号化され、前記保護情報は、暗号化された実データを復号するために必要な鍵であることを特徴とする請求項1に記載の記録装置。

【請求項4】 前記鍵は、所定の暗号方法で暗号化され、前記データ部分に、暗号化された鍵を復号するために必要な鍵をさらに収容することを特徴とする請求項3に記載の記録装置。

【請求項5】 前記鍵は、所定の暗号方法で暗号化され、前記記録手段は、暗号化された鍵を復号するために必要な鍵を収容したファイルをさらに前記記録媒体に記録することを特徴とする請求項3に記載の記録装置。

【請求項6】 前記保護情報は、前記実データに対し使用の開始の時を示す開始時および前記実データに対し使用の終了の時を示す終了時のうちの少なくとも1つを含むことを特徴とする請求項1に記載の記録装置。

【請求項7】 前記保護情報は、前記実データを再生することができ得る回数を制限する回数制限情報であることを特徴とする請求項1に記載の記録装置。

【請求項8】 前記保護情報は、前記実データを複製することができ得る回数を制限する複製制限情報であることを特徴とする請求項1に記載の記録装置。

【請求項9】 前記保護情報は、前記実データがオリジナルな実データであるか複製された実データであるかを識別する複製識別情報であることを特徴とする請求項1に記載の記録装置。

【請求項10】 前記データ部分に、前記保護情報が改ざんされたか否かを識別する改ざん識別情報をさらに収容することを特徴とする請求項1に記載の記録装置。

【請求項11】 データを書き換え可能な記録媒体に記録する記録方法において、

特殊なハードウェアを用いずに動画等を同期して再生するためのコンピュータソフトウェアにより取り扱うことができるファイル構造を持つように、前記データのデータ構造を変換するステップと、

前記ファイル構造に変換されたデータを前記記録媒体に記録するステップとを備え、

前記ファイル構造は、実データである第1データ単位と、複数の前記第1データ単位の集合としての第2データ単位と、複数の前記第1データ単位間の関係と第1データ単位の実データに関する属性とを管理する管理情報を記述するためのデータ部分とを有し、

前記データ部分に、前記第1データ単位に成立する無体財産権を保護するための保護情報を収容することを特徴とする記録方法。

【請求項12】 特殊なハードウェアを用いずに動画等を同期して再生するためのコンピュータソフトウェアにより取り扱うことができるファイル構造となるように変換された実データを記録する記録媒体であって、

前記ファイル構造は、実データである第1データ単位と、複数の前記第1データ単位の集合としての第2データ単位と、複数の前記第1データ単位間の関係と第1データ単位の実データに関する属性とを管理する管理情報を記述するためのデータ部分とを有し、

前記データ部分に、前記第1データ単位に成立する無体財産権を保護するための保護情報を収容することを特徴とする記録媒体。

【請求項13】 前記保護情報を、前記データ部分に収容する代わりに独立なファイルに収容し、前記データ部分には前記ファイルを指定する指定情報を収容することを特徴とする請求項12に記載の記録媒体。

【請求項14】 前記実データは、所定の暗号方法で暗号化され、前記保護情報は、暗号化された実データを復号するために必要な鍵であることを特徴とする請求項12に記載の記録媒体。

【請求項15】 前記鍵は、所定の暗号方法で暗号化され、前記データ部分に、暗号化された鍵を復号するために必要な鍵をさらに収容することを特徴とする請求項12に記載の記録媒体。

【請求項16】 前記保護情報は、前記実データに対し使用の開始の時を示す開始時および前記実データに対し使用の終了の時を示す終了時のうちの少なくとも1つを含むことを特徴とする請求項12に記載の記録媒体。

【請求項17】 前記保護情報は、前記実データを再生

することができ得る回数を制限する回数制限情報であることを特徴とする請求項１に記載の記録媒体。

【請求項１８】 前記保護情報は、前記実データを複製することができ得る回数を制限する複製制限情報であることを特徴とする請求項１に記載の記録媒体。

【請求項１９】 前記保護情報は、前記実データがオリジナルな実データであるか複製された実データであるかを識別する複製識別情報であることを特徴とする請求項１に記載の記録媒体。

【請求項２０】 前記データ部分に、前記保護情報が改ざんされたか否かを識別する改ざん識別情報をさらに収容することを特徴とする請求項１に記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、記録媒体に映像データやオーディオデータなどを記録する記録装置において、特に、記録媒体に記録されているこれらデータに成立する無体財産権などの権利を保護する機能を備える記録装置に関する。そして、このような記録装置に用いられる記録方法、および記録媒体に関する。

【０００２】

【従来の技術】映像データ、オーディオデータまたはコンピュータプログラムなどのデータは、記録媒体に製造工場で記録されて消費者に頒布されたり、通信回線を通じて記録媒体にダウンロードされて消費者に配布されたりする。

【０００３】記録媒体は、例えば、ＣＤ（compact disc）およびＤＶＤ（digital versatile discまたはdigital video disc）などの光ディスク、ＭＤなどの光磁気ディスクおよびメモリカードなどである。

【０００４】

【発明が解決しようとする課題】ところで、データの頒布・配布に際し、これらデータに成立する無体財産権、特に、著作権や特許権などを保護する必要がある。

【０００５】そこで、本発明は、データに成立する無体財産権を保護する機能を備えた記録装置を提供することを目的とする。

【０００６】さらに、本発明は、無体財産権を保護することができる記録方法、および、無体財産権を保護することができるようにデータが記録された記録媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明では、データを書き換え可能な記録媒体に記録する記録装置において、特殊なハードウェアを用いずに動画等を同期して再生するためのコンピュータソフトウェアにより取り扱うことができるファイル構造を持つように、前記データのデータ構造を変換する変換手段と、前記ファイル構造に変換されたデータを前記記録媒体に記録する記録手段とを備え、前記ファイル構造は、実データである第１データ単

位と、複数の前記第１データ単位の集合としての第２データ単位と、複数の前記第１データ単位間の関係と第１データ単位の実データに関する属性とを管理する管理情報を記述するためのデータ部分とを有し、前記データ部分に、前記第１データ単位に成立する無体財産権を保護するための保護情報を収容することで構成される。

【０００８】本発明では、このような記録装置において、保護情報を独立なファイルに収容し、前記データ部分には前記ファイルを指定する指定情報を収容するようにしても良い。

【０００９】本発明では、このような記録装置において、無体財産権を確実に保護する観点から、実データを所定の暗号方法で暗号化して、保護情報には、暗号化された実データを復号するために必要な鍵を含むようにすると好適であり、さらに、鍵自体を所定の暗号方法で暗号化し、データ部分に、暗号化された鍵を復号するために必要な鍵をさらに収容するようにすると好適である。

【００１０】本発明では、このような記録装置において、無体財産権を確実に保護する観点から、データ部分に、保護情報が改ざんされたか否かを識別する改ざん識別情報をさらに収容するようにすると好適である。

【００１１】本発明では、このような記録装置において、無体財産権を確実に保護する観点から、保護情報には、前記実データに対し使用の開始の時を示す開始時および前記実データに対し使用の終了の時を示す終了時のうちの少なくとも１つを含めたり、前記実データを再生することができ得る回数を制限する回数制限情報を含めたり、前記実データを複製することができ得る回数を制限する複製制限情報を含めたり、前記実データがオリジナルな実データであるか複製された実データであるかを識別する複製識別情報を含めたりすると好適である。

【００１２】このように本発明は、無体財産権を保護するための保護情報を記録媒体に記録された実データと関連付けて記録するので、実データを権利侵害から確実に保護することができる。さらに、第１データ単位ごとに保護情報を付するので、記録媒体ごとではなく、個々の実データごとに権利侵害から確実に保護することができる。このため、第１データ単位ごとに様々なサービスを提供することができる。

【００１３】

【発明の実施の形態】以下、本発明の実施形態について図面に基いて説明する。なお、各図において、同一の符号は、同一の構成であることを示す。

【００１４】図１は、デジタル記録再生装置の一構成例を示すブロック図である。

【００１５】図１において、デジタル記録再生装置は、ビデオ符号器１１、オーディオ符号器１２、ビデオ復号器１３、オーディオ復号器１４、ファイル生成器１５、ファイル復号器１６、メモリ１７、２０、メモリコントローラ１８、システム制御マイコン１９、エラー訂

正符号／復号器21、ドライブ制御マイコン22、データ変復調器23、磁界変調ドライバ24、操作部26、サーボ回路30、モータ31、磁界ヘッド32および光ピックアップ33を備えて構成される。

【0016】ビデオ信号は、ビデオ入力端子からビデオ符号器11に供給され、圧縮符号化される。オーディオ信号は、オーディオ入力端子からオーディオ符号器12に供給され、圧縮符号化される。ビデオ符号器11およびオーディオ符号器12の各出力がエレメンタリストームと呼ばれる。

【0017】本実施形態では、デジタル記録再生装置は、カメラ一体型デジタル記録再生装置に備えられているものとする。ビデオ信号は、ビデオカメラで撮影された画像が供給され、ビデオカメラは、光学系によって被写体の撮像光がCCD(ChargeCoupled Device)などの撮像素子に供給されることによってビデオ信号を生成する。オーディオ信号は、マイクロフォンで集音された音声供給される。

【0018】ビデオ符号器11は、例えば、圧縮符号化がMPEGの場合には、アナログ／デジタル変換器(A/D変換器)、フォーマット変換部、画像並替部、減算部、DCT部、量子化部、可変長符号化部、バッファメモリ、レート制御部、逆量子化部、逆DCT部、加算部、フレームメモリ、動き補償予測部およびスイッチの各電子回路を備えて構成される。

【0019】ビデオ符号器11に供給されたビデオ信号は、A/D変換器でデジタル化された後に、フォーマット変換部で符号化で用いる空間解像度に変換され、画像並替部に出力される。画像並替部は、ピクチャの順序を符号化処理に適した順に並び替える。画面並替部の出力は、減算部を介してDCT部に入力され、DCT符号化が行われる。DCT部の出力は、量子化部に入力され、所定のビット数で量子化される。量子化部の出力は、可変長符号化部および逆量子化部に入力される。可変長符号化部は、ハフマン符号などの可変長符号で符号化され、符号化データは、メモリのバッファメモリに出力される。バッファメモリは、一定レートで符号化データをビデオ符号器の出力として出力する。また、レート制御部は、可変長符号化部で発生する符号量が可変であるため、バッファメモリを監視することによって所定のビットレートを保つように、量子化部の量子化動作を制御する。

【0020】一方、IピクチャおよびPピクチャの場合は、動き補償予測部で参照画面として使用されるため、量子化部から逆量子化部に入力された信号は、逆量子化された後に逆DCT部に入力され、逆DCTが行われる。逆DCT部の出力は、加算部で動き補償予測部の出力と加算され、フレームメモリに入力される。フレームメモリの出力は、動き補償予測部に入力される。動き補償予測部は、前方向予測、後方向予測および両方向予測

を行い、加算部および減算部に出力する。これら逆量子化部、逆DCT部、加算部、フレームメモリおよび動き補償予測部は、ローカル復号部を構成し、ビデオ復号器と同一のビデオ信号が復元される。

【0021】減算部は、画像並替部の出力と動き補償予測部の出力との間で減算を行い、ビデオ信号とローカル復号部で復号された復号ビデオ信号との間の予測誤差を形成する。フレーム内符号化(Iピクチャ)の場合では、スイッチにより、減算部は、減算処理を行わず、単にデータが通過する。

【0022】図1に戻って、オーディオ符号器12は、例えば、MPEG/Audioレイヤ1/レイヤ2の場合では、サブバンド符号化部および適応量子化ビット割り当て部などの各電子回路を備えて構成される。オーディオ信号は、サブバンド符号化部で32帯域のサブバンド信号に分割され、適応量子化ビット割り当て部で心理聴覚重み付けに従って量子化され、ビットストリームに形成された後に出力される。なお、符号化品質を向上させるために、MPEG/Audioレイヤ3を適用しても良い。

【0023】ビデオ符号器11の出力およびオーディオ符号器12の出力がファイル生成器15に供給される。ファイル生成器15は、特定のハードウェア構成を使用することなく動画、音声およびテキストなどを同期して再生することができるコンピュータソフトウェアにより扱うことができるファイル構造を持つように、ビデオエレメンタリストリームおよびオーディオエレメンタリストームのデータ構造を変換する。このようなソフトウェアは、例えば、QuickTime(米Apple社が提供するクロスプラットフォームマルチメディアフォーマットの代表、以下、「QT」と略記する。)が知られている。以下、QTを使用する場合について説明する。ファイル生成器15は、システム制御マイコン19の制御下で符号化ビデオデータと符号化オーディオデータとを暗号化鍵で暗号化した後にこれらを多重化する。

【0024】暗号化アルゴリズムは、暗号化の単位を一定の単位長とする観点から、本実施形態では、ブロック暗号方式が好適であり、例えば、後述のDES、FEAL、MISTY、MULTI、IDEA、RC5などがある。

【0025】ファイル生成器15の出力であるQuickTimeムービーファイルは、メモリコントローラ18を介してメモリ17に順次書き込まれる。メモリコントローラ18は、システム制御マイコン19から記録媒体40へのデータ書き込みが要求されると、メモリ17からQuickTimeムービーファイルを読み出す。また、システム制御マイコン19は、プログラムを実行中に生じる各種データをメモリコントローラ18を介してメモリ17に格納する。

【0026】ここで、QuickTimeムービー符号化の転送



レートは、記録媒体40への書き込みデータの転送レートより低い転送レート、例えば、1/2に設定される。よって、QuickTimeムービーファイルが連続的にメモリ17に書き込まれるのに対し、メモリ17からのQuickTimeムービーファイルの読み出しは、メモリ17がオーバーフローまたはアンダーフローしないように、システム制御マイコン19によって監視されながら間欠的に行われる。

【0027】メモリ17から読み出されたQuickTimeムービーファイルは、メモリコントローラ18からエラー訂正符号/復号器21に供給される。エラー訂正符号/復号器21は、このQuickTimeムービーファイルを一旦メモリ20に書き込み、インターリーブ(interleave)およびエラー訂正符号の冗長データの生成を行う。エラー訂正符号/復号器21は、冗長データが付加されたデータをメモリ20から読み出し、これをデータ変復調器23に供給する。

【0028】データ変復調器23は、デジタルデータを記録媒体40に記録する際に、再生時のクロック抽出を容易とし、符号間干渉などの問題が生じないように、データを変調する。例えば、(1, 7) RLL (run length limited) 符号やトレリス符号などを利用することができる。

【0029】データ変復調器23の出力は、磁界変調ドライバ24および光ピックアップ33に供給される。磁界変調ドライバ24は、入力信号に応じて、磁界ヘッド32を駆動して記録媒体40に磁界を印加する。光ピックアップ33は、入力信号に応じて記録用のレーザービームを記録媒体40に照射する。このようにして、記録媒体40にデータが記録される。

【0030】記録媒体40は、ディスク状の記録媒体であり、例えば、光磁気ディスク(MO、magneto-optical disk)、相変化型ディスクなどの書き換え可能な光ディスクである。

【0031】本実施形態では、MO、例えば、直径約4cm、直径約5cm、直径約6.5cmまたは直径約8cmなどの比較的小径なディスクが使用される。記録媒体40は、モータ31によって、線速度一定(CLV、constant linear velocity)、角速度一定(CAV、constant angular velocity)またはゾーンCLV(ZCLV、zone constant linear velocity)で回転される。

【0032】ドライブ制御マイコン22は、システム制御マイコン19の要求に応じて、サーボ回路30に信号を出力する。サーボ回路30は、この出力に応じて、モータ31および光ピックアップ33を制御することによって、ドライブ全体を制御する。例えば、サーボ回路30は、光ピックアップ33に対し、記録媒体40の径方向の移動サーボ、トラッキングサーボおよびフォーカスサーボを行い、モータ31に対し、回転数を制御する。

【0033】また、システム制御マイコン19には、ユーザが所定の指示を入力する操作部26が接続される。

【0034】再生の際には、光ピックアップ33は、再生用の出力でレーザービームを記録媒体40に照射し、その反射光を光ピックアップ33内の光検出器で受光することによって、再生信号を得る。この場合において、ドライブ制御マイコン22は、光ピックアップ33内の光検出器の出力信号からトラッキングエラーおよびフォーカスエラーを検出し、読み取りのレーザービームがトラック上に位置し、トラック上に合焦するように、サーボ回路30によって光ピックアップ33を制御する。さらに、ドライブ制御マイコン22は、記録媒体40上における所望の位置のデータを再生するために、光ピックアップの径方向における移動も制御する。所望の位置は、記録時と同様にシステム制御マイコン19によって、ドライブ制御マイコン22に信号が与えられ、決定される。

【0035】光ピックアップ33の再生信号は、データ変復調器23に供給され、復調される。復調されたデータは、エラー訂正符号/復号器21に供給され、再生データを一旦メモリ20に格納し、デインターリーブ(deinterleaved)およびエラー訂正が行われる、エラー訂正後のQuickTimeムービーファイルは、メモリコントローラ18を介してメモリ17に格納される。

【0036】メモリ17に格納されたQuickTimeムービーファイルは、システム制御マイコン19の要求に応じて、ファイル復号器16に出力される。システム制御マイコン19は、ビデオ信号およびオーディオ信号を連続再生するために、記録媒体40の再生信号がメモリ17に格納されるデータ量と、メモリ17から読み出されてファイル復号器16に供給されるデータ量とを監視することによって、メモリ17がオーバーフローまたはアンダーフローしないようにメモリコントローラ18およびドライブ制御マイコン22を制御する。こうして、システム制御マイコン19は、記録媒体40から間欠的にデータを読み出す。

【0037】ファイル復号器16は、システム制御マイコン19の制御下で、QuickTimeムービーファイルをビデオエレメンタリストリームとオーディオエレメンタリファイルとに分離する。ファイル復号器16は、システム制御マイコン19の制御下で後述の権利保護情報および暗号化鍵に基づいてデータを復号する。ここで、権利保護情報の内容がデータの使用を禁止する場合、または、暗号化鍵が適正ではない場合には、データは、復号されない。復号されたビデオエレメンタリストリームは、ビデオ復号器13に供給され、圧縮符号化の復号が行われてビデオ出力となってビデオ出力端子から出力される。復号されたオーディオエレメンタリストリームは、オーディオ復号器14に供給され、圧縮符号化の復号が行われてオーディオ出力となってオーディオ出力端

子から出力される。ここで、ファイル復号器16は、ビデオエレメンタリストリームとオーディオエレメンタリストリームとが同期するように出力する。

【0038】ビデオ復号器13は、例えば、MPEGの場合では、メモリのバッファメモリ、可変長符号復号部、逆量子化部、逆DCT部、加算部、フレームメモリ、動き補償予測部、画面並替部およびデジタル／アナログ変換器（以下、「D/A」と略記する。）の各電子回路を備えて構成される。ビデオエレメンタリストリームは、一旦バッファメモリに蓄積され、可変長復号部に入力される。可変長復号部は、マクロブロック符号化情報が復号され、予測モード、動きベクトル、量子化情報および量子化DCT係数が分離される。量子化DCT係数は、逆量子化部でDCT係数に復元され、逆DCT部で画素空間データに変換される。加算部は、逆量子化部の出力と動き補償予測部の出力とを加算するが、Iピクチャを復号する場合には、加算しない。画面内のすべてのマクロブロックが復号され、画面は、画面並替部で元の入力順序に並べ替えられて、D/Aでアナログ信号に変換されて出力される。また、加算部の出力は、IピクチャおよびPピクチャの場合には、その後の復号処理で参照画面として使用されるため、フレームメモリに蓄積され、動き補償予測部に出力される。

【0039】オーディオ復号器14は、例えば、MPEG/Audioレイヤ1/レイヤ2の場合では、ビットストリーム分解部、逆量子化部およびサブバンド合成フィルタバンク部などの各電子回路を備えて構成される。入力されたオーディオエレメンタリストリームは、ビットストリーム分解部でヘッダと補助情報と量子化サブバンド信号とに分離され、量子化サブバンド信号は、逆量子化部で割り当てられたビット数で逆量子化され、サブバンド合成フィルタバンクで合成された後に、出力される。

【0040】このようなデジタル記録再生装置は、ビデオデータ、オーディオデータ、テキストデータおよびコンピュータプログラムなど、無体財産権（著作権や特許権など）が成立するデータを記録媒体40に記録する際に、無体財産権を保護するためのデータ（以下、「権利保護データ」と呼称する。）も記録される。そして、権利保護データは、デジタル記録再生装置がビデオデータなどの保護すべきデータと同様に扱えるように、保護すべきデータと同一のファイル形式で生成される。本実施形態では、保護すべきデータおよび権利保護データは、例えば、QuickTimeムービーファイルの形式で生成される。このため、記録再生装置は、すべてをQTで再生することができる。

【0041】QTは、各種データを時間軸に沿って管理するソフトウェアであり、特殊なハードウェアを用いずに動画や音声やテキストなどを同期して再生するためのOS拡張機能である。QTは、例えば、「INSIDE MACI

NTOSH :QuickTime（日本語版）（アジソンウエスレス）」などに開示されている。以下、この文献に沿って、QuickTimeムービーファイルについて概説する。

【0042】QTムービーリソースの基本的なデータユニットは、アトム (atom) と呼ばれ、各アトムは、そのデータとともに、サイズおよびタイプ情報を含んでいる。また、QTでは、データの最小単位がサンプル (sample) として扱われ、サンプルの集合としてチャンク (chunk) が定義される。

【0043】図2は、QuickTimeムービーファイルの構成例を示す図である。

【0044】図3は、ビデオメディア情報アトムの構成例を示す図である。図3は、図2におけるビデオメディア情報アトムをより詳細に示した図となっており、トラックがビデオ情報の場合について示している。

【0045】図2および図3において、QuickTimeムービーファイルは、大きく2つの部分、ムービーアトム (movie atom) 101およびムービー・データ・アトム (movie data atom) 102から構成される。ムービーアトム101は、そのファイルを再生するために必要な情報や実データを参照するために必要な情報を格納する部分である。ムービー・データ・アトム102は、ビデオデータ、オーディオデータ、コンピュータプログラムおよびテキストデータなどの実データを格納する部分である。

【0046】ムービーアトム101は、ムービー全体に関する情報を収容するムービー・ヘッダ・アトム (movie header atom) 111、クリッピング領域を指定するムービー・クリッピング・アトム (movie clipping atom) 112、ユーザ定義データアトム113、および、1または複数のトラックアトム (track atom) 114などを含む。

【0047】トラックアトム114は、ムービー内の1つのトラックごとに用意される。トラックアトム114は、トラック・ヘッダ・アトム (track header atom) 131、トラック・クリッピング・アトム (track clipping atom) 132、トラック・マット・アトム (track matte atom) 133、エディットアトム (edit atom) 134およびメディアアトム (media atom) 135に、ムービー・データ・アトム102の個々のデータに関する情報を記述する。図2では、1つのビデオムービーのトラックアトム114-1が示され、他のトラックアトムは、省略されている。

【0048】メディアアトム135は、メディア・ヘッダ・アトム (media header atom) 144、メディア情報アトム (media information atom) (図2および図3では、ビデオメディア情報アトム145)、および、メディア・ハンドラ・リファレンス・アトム (media handler reference atom) 146に、ムービートラックのデータやメディアデータを解釈するコンポーネントを規定

する情報などを記述する。

【0049】メディア・ハンドラは、メディア情報アトムの情報を使用して、メディア時間からメディアデータへのマッピングを行う。

【0050】メディア情報アトム145は、データ・ハンドラ・リファレンス・アトム (data handler reference atom) 161、メディア情報ヘッダ・アトム (media information header atom) 162、データ情報アトム (data information atom) 163およびサンプル・テーブル・アトム (sample table atom) 164を含む。

【0051】メディア情報ヘッダ・アトム (図3では、ビデオ・メディア情報ヘッダ・アトム162) は、メディアにかかる情報が記述される。データ・ハンドラ・リファレンス・アトム161は、メディアデータの取り扱いにかかる情報が記述され、メディアデータへのアクセス手段を提供するデータ・ハンドラ・コンポーネントを指定するための情報が含まれる。データ情報アトム163は、データ・リファレンス・アトム (data reference atom) を含み、データについての情報が記述される。

【0052】サンプル・テーブル・アトム164は、メディア時間を、サンプル位置を指すサンプル番号に変換するために必要な情報を含む。サンプル・テーブル・アトム164は、サンプル・サイズ・アトム (sample size atom) 172、時間サンプルアトム (time-to-sample atom) 173、同期サンプルアトム (sync sample atom) 174、サンプル・ディスクリプション・アトム (sample description atom) 175、サンプル・チャンク・アトム (sample-to-chunk atom) 176、チャンク・オフセット・アトム (chunk offset atom) 177、および、シャドウ同期アトム (shadow sync atom) 178で構成される。

【0053】サンプル・サイズ・アトム172は、サンプルの大きさが記述される。時間サンプル・アトム173は、何秒分のデータが記録されているか?という、サンプルと時間軸との関係が記述される。同期サンプルアトム174は、同期にかかる情報が記述され、メディア内のキーフレームが指定される。キーフレームは、先行するフレームに依存しない自己内包型のフレームである。サンプル・ディスクリプション・アトム175は、メディア内のサンプルをデコード (decode) するために必要な情報が保存される。メディアは、当該メディア内で使用される圧縮タイプの種類に応じて、1つまたは複数のサンプル・ディスクリプション・アトムを持つことができる。サンプル・チャンク・アトム176は、サンプル・ディスクリプション・アトム175内のテーブルを参照することで、メディア内の各サンプルに対応するサンプル・ディスクリプションを識別する。サンプル・チャンク・アトム176は、サンプルとチャンクとの関係が記述され、先頭チャンク、チャンク当たりのサンプル数およびサンプル・ディスクリプションID (sample

description-ID) の情報を基に、メディア内におけるサンプル位置が識別される。チャンク・オフセット・アトム177は、ムービーデータ内でのチャンクの開始ビット位置が記述され、データストリーム内の各チャンクの位置が規定される。

【0054】また、ムービー・データ・アトム102には、図2では、例えば、所定の圧縮符号化方式によって符号化されたオーディオデータ、および、所定の圧縮符号化方式によって符号化された画像データがそれぞれ所定数のサンプルから成るチャンクを単位として格納される。なお、データは、必ずしも圧縮符号化する必要はなく、リニアデータを格納することもできる。そして、例えば、テキスト・データやMIDIなどを扱う場合には、ムービー・データ・アトム102にテキストやMIDIなどの実データが含まれ、これに対応して、ムービーアトム101にテキストトラックやMIDIトラックなどが含まれる。

【0055】ムービーアトム101における各トラックアトム114と、ムービー・データ・アトム102に格納されているデータ (データストリーム) とは、唯一一つに対応付けられている。このような特徴的な構造をもつことによって、データ実体そのものに手を加えずに再生同期のスケジューリングや編集 (非破壊編集)、トラックの追加や削除が容易に実現することができる。

【0056】このような階層構造において、QTは、ムービー・データ・アトム102内のデータを再生する場合に、ムービーアトム101から順次に階層を辿り、サンプル・テーブル・アトム164内の各アトム172～178を基に、サンプル・テーブルをメモリに展開して、各データにおけるデータの解釈方法・属性など、および、各データ間の関係 (データの位置やデータのサイズなど) を識別する。そして、QTは、各データ間の関係を基にデータを再生する。

【0057】本実施形態は、QTの優れた特徴を生かしつつ、権利保護すべきデータを扱う際に必要となる機能やフォーマット上の構造を拡張することによって、データに成立する無体財産権を保護する。以下、無体財産権のうち、著作権について説明するが、他の無体財産権についても同様に扱うことができる。QT上の最少アクセス単位と言えるサンプルに、暗号化された実データの復号化可能な最少単位 (データブロック) を対応させることにより、QTの持つタイムベースでの管理能力を使って再生同期や編集などが行え、そして、鍵マネジメントとの組み合わせにおいては同一コンテンツ内においてもより細かく権利の付加や権利の利用条件の設定など、新たなコンテンツの運用を行うことができる。

【0058】より具体的には、本発明は、QTで権利保護されたマルチメディアコンテンツを扱う際に、暗号化されたデータを解くための鍵情報とコンテンツの使用条件などの権利保護のための情報を、それぞれのデータス

トリームに対応した形で確保するために、各トラックアトム内のサンプルディスクリプションテーブルに権利保護データを格納する拡張フォーマットを備えて構成される。

【0059】図4は、本実施形態のQuickTimeムービーファイルの構成を示す図である。

【0060】図5は、本実施形態のサンプル・ディスクリプション・テーブルの構成を示す図である。

【0061】図4に示すように、権利保護情報ブロック (Security Information Block) 191は、標準QTのフィールドに続いて拡張されるフィールドであり、各トラックのサンプル・ディスクリプション・テーブル内に設けられる。そして、権利保護情報ブロック191は、図5に示すように、権利管理データ (Rights Management Data、以下、「RMD」と略記する。) ユニット単独で、あるいはRMDユニットとその他のユニット (other unit) との複数ユニットから構成される。なお、各ユニットの格納順は、任意である。

【0062】ユニット・サイズ (unit size) ・フィールドは、それぞれのユニットに含まれ、そのユニットのバイト数を示す。ユニット・タイプ (unit type) ・フィールドは、そのユニットのタイプを指定するタグであり、ここでは、例えば、RMDユニット場合 right と定義する。

【0063】バージョン (version) ・フィールドは、それぞれのユニットのバージョンを表す値である。フラグ (Flag) ・フィールドは、このユニットに付属するフラグ用として予約されている。

【0064】フラグ・フィールドに続いて、そのユニットのデータ実体 (unit data) が格納される。RMDユニットでは、権利保護や暗号化鍵に関する情報をまとめたRMDのデータ実体となる。

【0065】なお、この拡張に応じて、標準QTのフィールド部分でこのテーブル内のデータタイプを指定しているデータ・フォーマット・フィールドが値として採るタグも、導入する権利保護システム、ファイルフォーマットなどに応じて新しく定義する必要がある拡張して定義することができる。

【0066】標準QTとは、本発明にかかる権利保護のために拡張したフィールドをサンプル・ディスクリプション・テーブルに備えないQTである。

【0067】図6は、権利管理データの構成を示す図である。

【0068】図6において、RMDユニットは、コンテンツの暗号化鍵 (content key、以下、「CK」と略記する。)、C\_MAC、RMF、PPN、プレイバック・カウンタ (playback counter)、使用開始日時 (start time/date)、使用終了日時 (end time/date)、CCF、PCN、複製カウンタ (copy counter)、予約領域 (reserved) など、各種使用条件などの著作権保護のた

めの情報がまとめて格納される。

【0069】CK・フィールドは、このトラックが対応するデータストリーム (詳細には、さらにトラックを細分化した各データブロック) を暗号化する際に使用されたコンテンツの暗号化鍵である。

【0070】C\_MAC・フィールドは、RMDを対象とした改ざん防止コードが格納される。これは、例えばISO/IEC9797のMAC (message authentication code) 演算手法によって、RMDの全フィールドの値を入力として得られた、一意に生成され非可逆の性質をもつ演算値である。

【0071】RMF (rights management flag) ・フィールドは、制限事項の有無と種類を示すフラグである。

【0072】PPN (number of permitted playback) ・フィールドは、再生可能回数の最大値である。

【0073】プレイバック・カウンタ・フィールドは、再生毎にデクリメントされる再生回数のカウンター値であり、初期値はPPN・フィールドと同値である。

【0074】使用開始日時・フィールドは、RMF・フィールドによって再生期限による制限事項が設定されている場合にその開始日時を表す。

【0075】使用終了日時・フィールドは、RMF・フィールドによって再生期限による制限事項が設定されている場合にその終了日時を表す。

【0076】CCF (copy control flag) ・フィールドは、複製制御用フラグであり、コピーが可能であるか/不可能であるかの別や、コピー可能な世代であるか、オリジナルであるか/複製であるかなどの当該データの属性を指定する。

【0077】PCN・フィールドは、例えば、LCM (Licensed Compliant Module) などとメディア間で許される、コンテンツの移動/複製可能回数の最大値を表す。

【0078】複製カウンタ・フィールドは、コンテンツ移動/コピーごとにデクリメントされるカウンター値であり、初期値はPCN・フィールドと同値である。

【0079】これらRMF、PPN、プレイバック・カウンタ、使用開始日時、使用終了日時、CCF、PCNおよび複製カウンタは、そのコンテンツの利用条件を指定する。

【0080】次に、図7および図8に基づいて、ムービー・データ・アトムの構成および実データとメディア・アトムとの対応付けについて説明する。

【0081】図7は、ムービー・データ・アトムの構成を示す図である。

【0082】図8は、実データとメディア・アトムとの対応を示す図である。

【0083】図7において、ムービーデータは、アトム・サイズ (atom size)、タイプ (type) およびデータから構成されるアトムである。図7に示す、サイズとタイプに続くデータ部分が、コンテンツの実データ (データ

ストリーム)である。

【0084】図7の権利保護データ (Secured Content Data) は、例えば、米国標準暗号方式であるDES (Data Encryption Standard) のブロック暗号化アルゴリズムによって暗号化される。ブロック暗号化は、一般的にデータをある程度の塊(ブロック)ごとに暗号化するとともに、ある程度の時間ごとに暗号化鍵を変更する。同一鍵で暗号化された暗号化データを一塊とし、復号化するために必要な情報をヘッダ情報として付加してブロック化したものを、暗号化データブロック (Encrypted Data Block) と呼称することにする。すなわち、暗号化データブロックは、鍵があればそれ単独で復号化できる、復号化最少単位である。暗号化されたデータストリーム (Encrypted Data Block #1 ~ Encrypted Data Block #n) は、この暗号化データブロックが連続したものである。

【0085】以下、特に断りがない場合はブロックとは暗号化データブロックを指すものとする。暗号化データブロックは、BLK ID、CONNUM、BLK Serial No.、Block SeedおよびEncrypted Dataとを備えて構成される。

【0086】BLK ID・フィールドは、ブロックの先頭を識別するコードを表す。

【0087】CONNUM・フィールドは、コンテンツをユニークにする識別子IDであり、あるコンテンツにおいて一定の値である。コンテンツが編集された場合でも、CONNUM・フィールドの値は、変化させず、各ブロックがどのコンテンツを構成していたものであるかを特定する情報となる。

【0088】BLK Serial No.・フィールドは、あるコンテンツの先頭ブロックを0とし、続くブロックに連続して昇順につけられていくブロック番号である。

【0089】Block Seed・フィールドは、該当ブロックを暗号化するための一種の鍵であり、ブロックごとに異なる。一般的に、コンテンツの暗号化鍵をコンテンツに対して唯一つにするため、実際にデータを暗号化する鍵は、コンテンツの暗号化鍵とこのBlock

Seedを組み合わせたものである。これによって、コンテンツの暗号化鍵が唯一つだとしても、同一コンテンツ内で所定の時間ごとに暗号化鍵が変化していく。組み合わせ方や暗号化鍵を変化させる時間間隔などは、暗号化アルゴリズムやシステムに依存する。

【0090】続くEncrypted Dataは、暗号化されたデータの実体が格納される。1つのブロックは、例えば、動画であれば1フレーム、音声であれば1〜数サウンドフレームなどのデータストリーム上の単位に相当させる。

【0091】図8において、QT上での最少アクセス単位であるサンプルを、一つの暗号化データブロックと対

応させる。これによって、例えば、暗号化データブロックを動画の1フレームに相当させた場合に、QTは、1フレーム単位でアクセス/再生したり、他のトラックと1フレーム精度で同期をとることができる。また、これによって、1フレーム精度での分割や結合、入れ替えなどの編集性も確保される。先に説明したサンプル・ディスクリプション・テーブルの構成から、1つのサンプル、もしくは複数のサンプルごとに使用条件やコンテンツの暗号化鍵などの著作権情報を設定することも可能となる。

【0092】データの保護は、データの暗号化、データの改ざん防止および暗号化鍵の管理の3段階で行われ、より多くの段階を用いることで保護が強化される。上述の実施形態は、データの暗号化にDESを適用し、改ざん防止にC\_MACを適用している。そこで、データ保護の強化を図るため、上述の実施形態に更に暗号化鍵の管理を用いると好適である。以下、暗号化鍵の管理手法も用いる実施形態について説明する。

【0093】図9は、暗号化鍵の管理を用いた場合におけるサンプル・ディスクリプション・テーブルの構成を示す図である。

【0094】図9において、サンプル・ディスクリプション・テーブルは、標準QTのフィールドに続いて拡張される権利保護情報ブロックとして、Enable Key Block (以下、「EKB」と略記する。)・ユニットと、RMD・ユニットとを拡張する。EKB・ユニットには、EKBと呼ばれるコンテンツの暗号化鍵を導くために必要な鍵や鍵束、および付随する属性情報などが格納される。

【0095】EKB・ユニットにおけるユニット・サイズ (unit size)・フィールドは、EKB・ユニット全体のバイト数を示す。ユニット・タイプ (unit type)・フィールドは、ユニットのタイプを指定するタグで、ここでは、例えば ekbl と定義される。EKB・ユニットにおけるバージョン (version)・フィールドは、それぞれのユニットのバージョンを表す値である。EKB・ユニットにおけるフラグ (flag)・フィールドは、ユニットのデータ本体(EKB)の有無と、参照方法を指定する。

【0096】EKB・ユニットにおけるEKB・フィールドは、フラグの状態値によって、EKBデータの実体か、もしくはファイルIDやファイル名、URLなどのリンク情報、またはデータ無し(EKB・フィールドが存在しない)の各状態を取り得る。EKBは、データストリームと基本的に一対で、一つのコンテンツを形成する。ここで、EKBの実体は、必ずしもムービー・アトム(リソース)の中に保持する必要はなく、例えば、同一記録媒体上に独立したファイルとして保持し、EKBファイルへのリンク情報によって必要なときに参照するようにしてもよい。また、複数コンテンツが同じEKBを使用すると場合のようにEKBが重複している場合な

どは、積極的にこのような独立したファイルとすることで記録媒体の容量に関して利用効率を向上することができる。さらに、コンテンツ提供者の意図によっては、コンテンツの配信時にはEKBと一対ではない状態でデータストリームのみを配信することもできる。このようにデータストリームのみを配信する場合に、例えば、EKBの取得先をインターネット上のURLによって指定することによって、後日に必要に応じてEKBを取得するようなサービス形態を提供することもできる。

【0097】図10は、EKB・ユニットにおけるフラグの定義を示す図である。

【0098】図10において、フラグ値0X00は、EKBデータが存在せず有効でないことを示す。フラグ値0X01は、EKBデータが存在しEKBユニット内に格納されていることを示す。フラグ値0X02は、EKBデータがEKB・ユニット内に存在しないが、同一記録媒体上などに独立ファイルとして存在し、ファイルIDおよびファイル名などの参照先情報によって参照可能であることを示す。フラグ値0X03は、EKBデータがEKB・ユニット内に存在しないが、インターネット上の取得先を指定するURL情報によって、EKBを取得することが可能であることを示す。その他のフラグ値は予約されている。

【0099】また、EKBを外部参照する場合には、図11に示すように、EKBは、独立したファイルとして構成させ、EKBの実体とともにいくつかのムービーからリンクされているかを示すリンク・カウンタ(Link Counter)や、バージョン、サイズなどの情報を付加させることで各コンテンツ(トラック)とEKBとの相関関係を管理する。

【0100】また、この拡張に応じて、図9における標準QTのフィールド部分でこのテーブル内のデータタイプを指定しているデータ・フォーマット(Data Format)・フィールドが値としてとるタグも、拡張の必要があれば、新たに拡張定義する。

【0101】図12は、EKBのデータ構造を示す図である。

【0102】図12は、上述のフラグ・フィールドにおいて、EKBが存在し実体がユニット内に格納されていると指定した場合に格納されるEKBの実体の例である。

【0103】図12において、バージョン(version)・フィールドは、このEKBのバージョンを表す値である。暗号化アルゴリズム(encryption algorithm)・フィールドは、EKBを構成する各々の暗号化鍵情報の暗号化に使用された暗号化アルゴリズムを指定する。Aをnという鍵で暗号化した結果のデータをE<sub>n</sub>(A)と表記する場合、E<sub>kr</sub>oot(KEK)は、K<sub>root</sub>という鍵を使って暗号化された鍵暗号化鍵(KEK=Key Encryption Key)である。KEKは、データストリームの

復号化に必要なコンテンツの暗号化鍵(KC)を導きだすのに必要な鍵である。つまり、本来、CK=E<sub>KEK</sub>(コンテンツの暗号化鍵(KC))である。

【0104】シグニチャ・パート(signature part)は、このEKBに対する電子署名である。続くフィールドは、最も下位階層の鍵から順に、すぐ上位の鍵を下位の鍵によって暗号化した鍵情報が連続する。最も下位階層の鍵とは、リーフ鍵(例えば、K<sub>leaf</sub>などと表される)と呼ばれる、メディアや機器がユニークに保持する鍵であり、正規なメディアや機器であればEKBを用いてKEKが導き出せることになる。

【0105】このようなファイルを対応アプリケーションQTによって再生する場合について以下に説明する。

【0106】ムービーを表示しようとする際に、システム制御マイコン19は、ファイル復号器16を介して、特定の時間に対応するメディアデータにアクセスする。システム制御マイコン19は、サンプル・テーブル・アトムの情報によって、要求されたサンプルに対応するデータストリームの位置を特定する。システム制御マイコン19は、同様に、そのサンプルを解釈するためのサンプル・ディスクリプション・テーブルを参照し、拡張されたEKB・ユニットのフラグ・フィールドによってEKBデータの属性を判断する。EKBデータが存在し実体が格納されている場合には、システム制御マイコン19は、続くEKBフィールドをEKBデータとして参照する。EKBデータが独立ファイルとして存在する場合は、システム制御マイコン19は、EKBフィールドに示されたリンク情報により、該当するEKBファイルを特定する。EKBフィールドがURLであった場合には、システム制御マイコン19は、URLで指定されたHPを参照し、そこから必要なEKBデータをダウンロードする。一方、EKBが存在しないなど、このコンテンツに対して使用権利が与えられていない場合は、システム制御マイコン19は、再生不可である旨や、EKBの取得を促すメッセージなど、必要に応じた処理をする。これによって得られたEKBと、そのアプリケーションがユニークに持つリーフ鍵から、システム制御マイコン19は、コンテンツの暗号化鍵を導くためのKEKを得ることができる。そして、システム制御マイコン19は、KEKとRMDから復号化するためのコンテンツの暗号化鍵を導き、さらに各種使用条件などの情報を判断する。システム制御マイコン19は、使用条件に応じた処理を行い、導かれたコンテンツの暗号化鍵と暗号化データブロック内のBlock Seedからこのブロックをファイル復号器16を介して復号化する。復号化されたデータストリームは、対応するコーデックを用いて伸張され、ビデオ復号器表示される。

【0107】次に、権利保護方法と提供されるサービスとの関係について説明する。

【0108】図13は、権利保護方法と提供されるサー

ビスとの第1の関係を説明する図である。

【0109】図13において、複数トラックが用意され、各トラックにコンテンツの内容は、同一であるが品質（解像度、音質など）の異なるデータを収容し、それぞれのサンプル・ディスクリプション・テーブルに異なった著作権情報を付加する。そして、額の異なる利用料金を設定し、支払われた利用料金額に応じた著作権保護情報およびコンテンツの暗号化鍵をユーザに提供するようにする。このようにすることで、利用料金に応じた品質のコンテンツを提供することができる。

【0110】例えば、トラック1は、第1の解像度のコンテンツを収容し、これに対応する著作権情報Aおよびコンテンツの暗号化鍵Aをサンプル・ディスクリプション・テーブルに収容する。そして、トラック2は、第1の解像度よりも高解像度でコンテンツを収容し、これに対応する著作権情報Bおよびコンテンツの暗号化鍵Bをサンプル・ディスクリプション・テーブルに収容する。このような場合に、初期料金が支払われた場合には、著作権情報AのEKBおよびコンテンツの暗号化鍵Aのうちユーザに提供していない一方または両方をユーザに提供してトラック1を再生することができるようにする。さらに、ユーザが初期料金に上乗せして支払う特別料金を支払った場合には、著作権情報BのEKBおよびコンテンツの暗号化鍵Bのうちユーザに提供していない一方または両方をユーザに提供してトラック2を再生することができるようにする。

【0111】あるいは、異なる額の利用料金を設定して購入時の金額に応じて、ユーザに、著作権情報AのEKBおよびコンテンツの暗号化鍵Aのうちユーザに提供していない一方または両方、あるいは、著作権情報BのEKBおよびコンテンツの暗号化鍵Bのうちユーザに提供していない一方または両方を提供するようにする。これによって利用料金の額に応じた解像度のコンテンツを提供することができる。このように利用料金に応じてスケラビリティを持つコンテンツを提供することができる。

【0112】また、同様に、それぞれのトラックを異なるデータ、例えば、映像データおよび音楽データとすることで、例えば、音楽配信サービスにおいて購入した楽曲に対して特別料金を払うことでビデオクリップコンテンツになったり、カラオケコンテンツになったりなど、多様なサービスに対応できる。

【0113】図14は、権利保護方法と提供されるサービスとの第2の関係を説明する図である。

【0114】図14において、一個のトラックは、暗号化されたブロックと暗号化されないブロックとで構成される。暗号化されたブロックに対応するサンプル・ディスクリプション・テーブルには、その著作権情報を格納する。

【0115】このような形態によって、例えば、音楽配

信サービスにおいて、次のようなサービスを実現することができる。すなわち、ある楽曲の中でサビの部分などコンテンツ提供者側が意図した部分のみを暗号化しないブロックとして構成することで、ユーザは、無料でその楽曲の一部を試聴することができ、購入を希望する場合にはコンテンツ鍵を別途購入（そのコンテンツ鍵を導けるEKBデータを購入）する。この購入によって、ユーザは、その時点で楽曲全てを楽しむことができるようになる。

【0116】図15は、権利保護方法と提供されるサービスとの第3の関係を説明する図である。

【0117】図15において、一個のトラックは、いくつかのブロックに分けられ、それぞれ異なるコンテンツの暗号化鍵で暗号化される。それぞれのブロックに対応するサンプル・ディスクリプション・テーブルには、それぞれの著作権情報を格納する。

【0118】このような形態によって、例えば、動画配信サービスにおいて、次のようなサービスを実現することができる。すなわち、連続的なコンテンツを著作権者の意向に合わせて細かく切り売りすることができる。また、鍵は同じであっても再生期限などの使用条件を変えて、連続ドラマのようなコンテンツを意図したタイミングで次々に公開（再生許可）することもできる。

【0119】そして、これらの組み合わせによって、一つのコンテンツの中でより複雑な使用条件などを設定することができるので、より細かな、新しいコンテンツサービスを展開することができる。

【0120】ここで、従来は、コンテンツとコンテンツを利用するための鍵とを一体に扱っていたので、ユーザには、ユーザの希望するコンテンツのみしか提供することができなかった。

【0121】本発明を利用すれば、コンテンツとコンテンツを利用するために必要な著作権情報のEKBおよびコンテンツの暗号化鍵とを別個に管理することができる。このため、ユーザに頒布する際には、複数のコンテンツを記録した記録媒体を予め頒布したり、複数のコンテンツを通信回線を通じて予め配布することができる。すなわち、ユーザが初期に希望しないコンテンツも提供することができる。

【0122】これによって、ユーザが初期に希望したコンテンツにさらに別のコンテンツを希望する場合には、ユーザが希望するコンテンツにおける著作権情報のEKBおよびコンテンツの暗号化鍵のうちのユーザに提供していない一方または両方をユーザに提供するだけで、ユーザは、希望するコンテンツを利用することができる。

【0123】したがって、著作権情報のEKBやコンテンツの暗号化鍵と言った最小のデータのみをユーザに提供すればよい。このような最小のデータを通信回線を通じて提供する場合には、コンテンツとともに提供する従来の場合に較べ格段に短い通信時間で提供することがで

き、ユーザのダウンロードに伴うストレスや通信料金の高額化を避けることができる。

【0124】なお、本発明に係るファイルを記録した記録媒体は、Q Tを搭載したコンピュータによって読み取り可能である。また、コンテンツを復号するための暗号化鍵が記録媒体に記録されない場合であって、コンピュータにモデムなどの通信用インターフェースが搭載され通信回線に接続可能である場合には、暗号化鍵は、通信回線を介して取得することが可能である。これによって、実データと実データを使用する権利とを別個に販売することが可能である。

【0125】

【発明の効果】本発明によれば、特殊なハードウェアを用いずに動画等を同期して再生するためのコンピュータソフトウェアにより取り扱うことができるファイル構造を持つようにデータ構造が変換された実データに成立する無体財産権を確実に保護することができる。

【0126】そして、本発明によれば、権利保護の単位を第1データ単位ごとに合わせたので、データ提供者が意図した単位で、ユーザにアクセス、再生、同期および編集などを行わせることができる。

【図面の簡単な説明】

【図1】ディジタル記録再生装置の一構成例を示すブロック図である。

【図2】QuickTimeムービーファイルの一構成例を示す図である。

【図3】ビデオメディア情報アトムの一構成例を示す図である。

【図4】本実施形態のQuickTimeムービーファイルの構成を示す図である。

【図5】本実施形態のサンプル・ディスクリプション・テーブルの構成を示す図である。

【図6】権利管理データの構成を示す図である。

【図7】ムービー・データ・アトムの構成を示す図である。

【図8】実データとメディア・アトムとの対応を示す図である。

【図9】暗号化鍵の管理を用いた場合におけるサンプル・ディスクリプション・テーブルの構成を示す図であ

る。

【図10】E K B・ユニットにおけるフラグの定義を示す図である。

【図11】権利保護情報ブロックを独立ファイルとした場合を説明する図である。

【図12】E K Bのデータ構造を示す図である

【図13】権利保護方法と提供されるサービスとの第1の関係を説明する図である。

【図14】権利保護方法と提供されるサービスとの第2の関係を説明する図である。

【図15】権利保護方法と提供されるサービスとの第3の関係を説明する図である。

【符号の説明】

- 11 ビデオ符号器
- 12 オーディオ符号器
- 13 ビデオ復号器
- 14 オーディオ復号器
- 15 ファイル生成器
- 16 ファイル復号器
- 17、20 メモリ
- 18 メモリコントローラ
- 19 システム制御マイコン
- 21 エラー訂正符号／復号器
- 23 データ変復調器
- 24 磁界変調ドライバ
- 26 操作部
- 30 サーボ回路
- 31 モータ
- 32 磁界ヘッド
- 33 光ピックアップ
- 40 記録媒体
- 103 E K B・ファイル
- 104 リンク・カウンタ
- 105 E K B・データ
- 175 サンプル・ディスクリプション・アトム
- 181、182 サンプル・ディスクリプション・テーブル
- 191 権利保護情報ブロック

【図6】

Rights Management Data	
Content Key (CK)	
C MAC	
RMP	
PPN	
Playback Counter	
Start time/date	
End time/date	
CCP	
PCN	
Copy Counter	
reserved	

【図10】

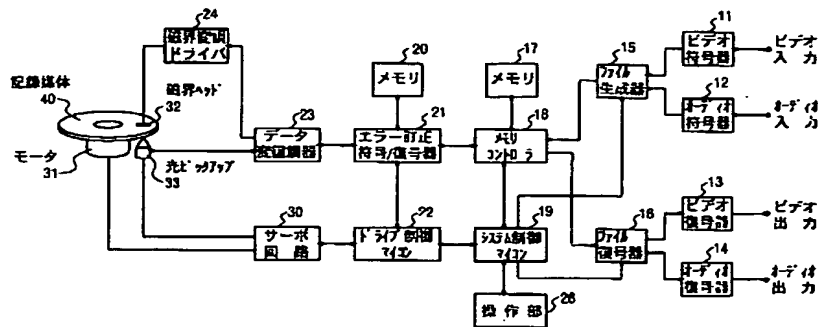
Flag	Attribute		EKB field
0x00	not-exist	non-valid	No data
0x01	exist	valid	EKB data
0x02	not-exist	valid as independent file	Link information (File ID, File name and etc.)
0x03	not-exist	valid on Internet	Link information (URL and etc.)
others			reserved

【図12】

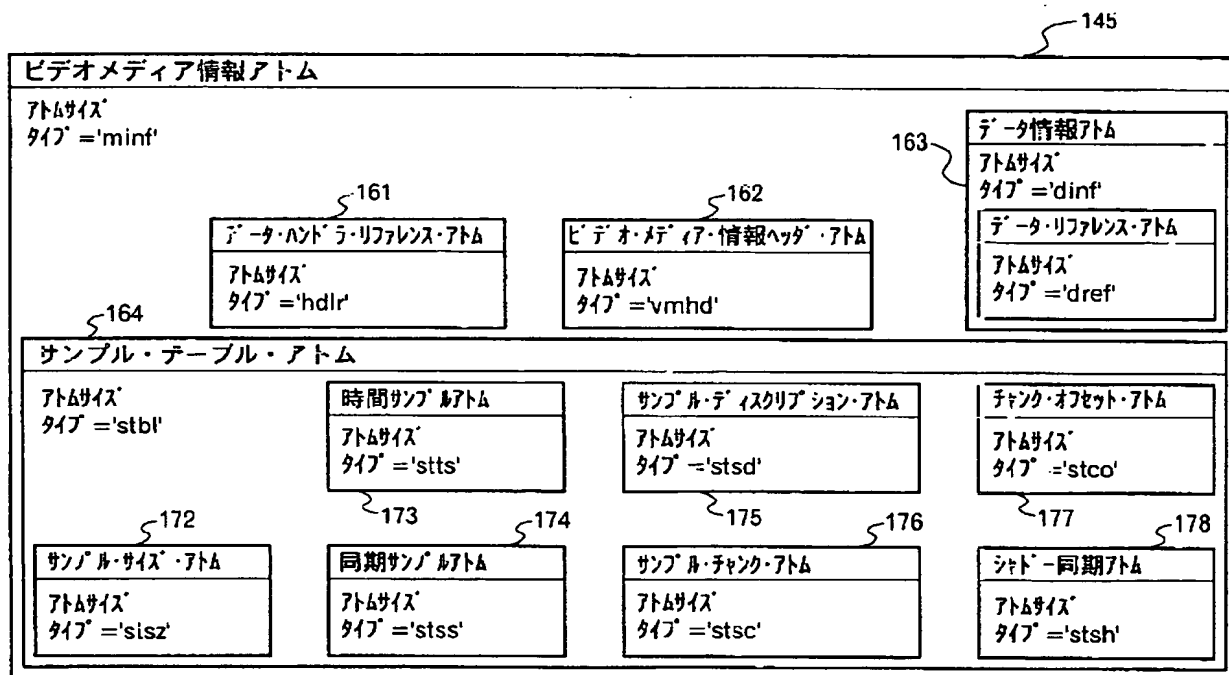
Enable Key Block	
Version	
Encryption Algorithm	
Encr(KEK)	
Signature Part	
Enc(Kroot)	
Enc(KD)	
Enc(KI)	
...	
Enc(Kn-1)	
Enc(Kn)	



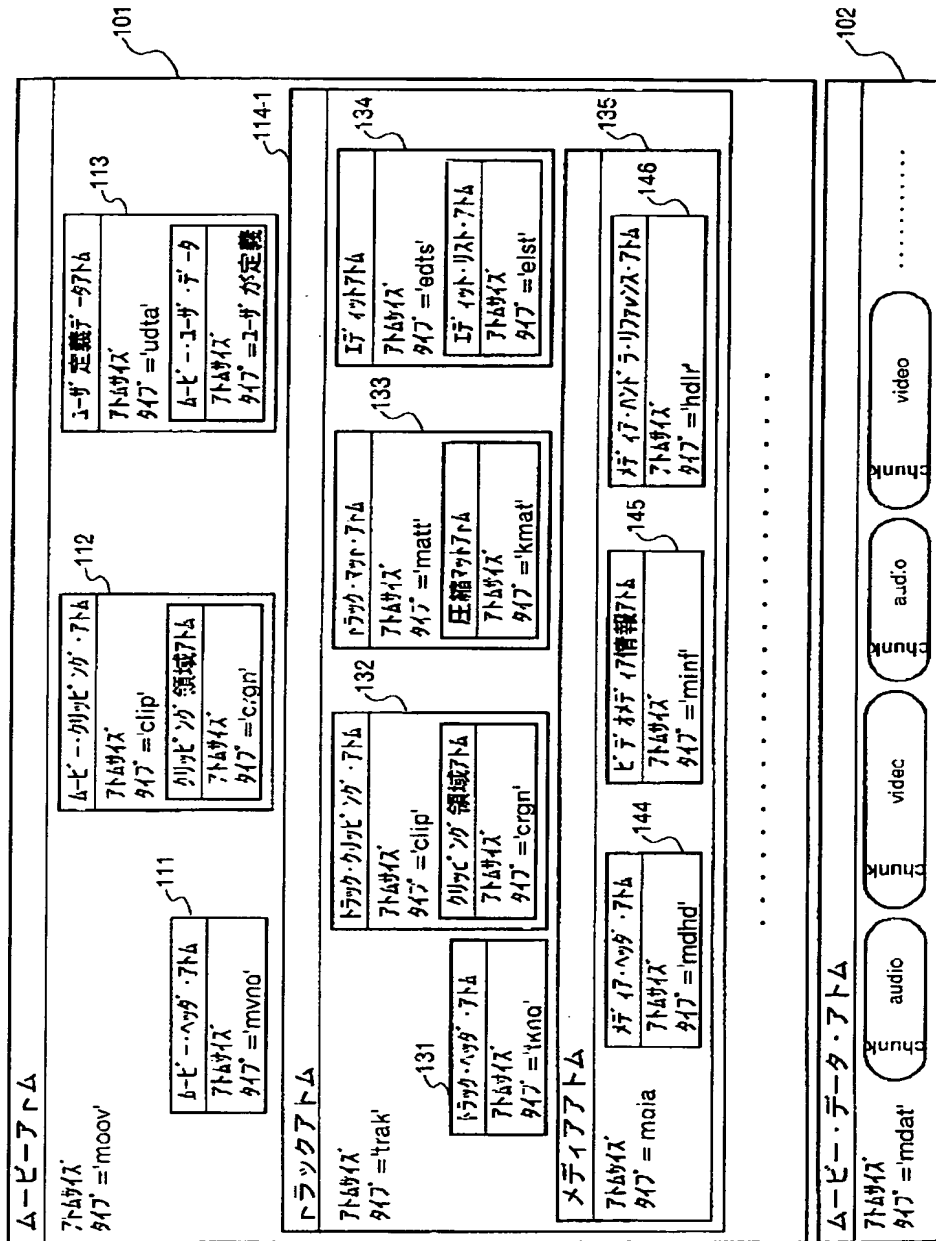
【図 1】



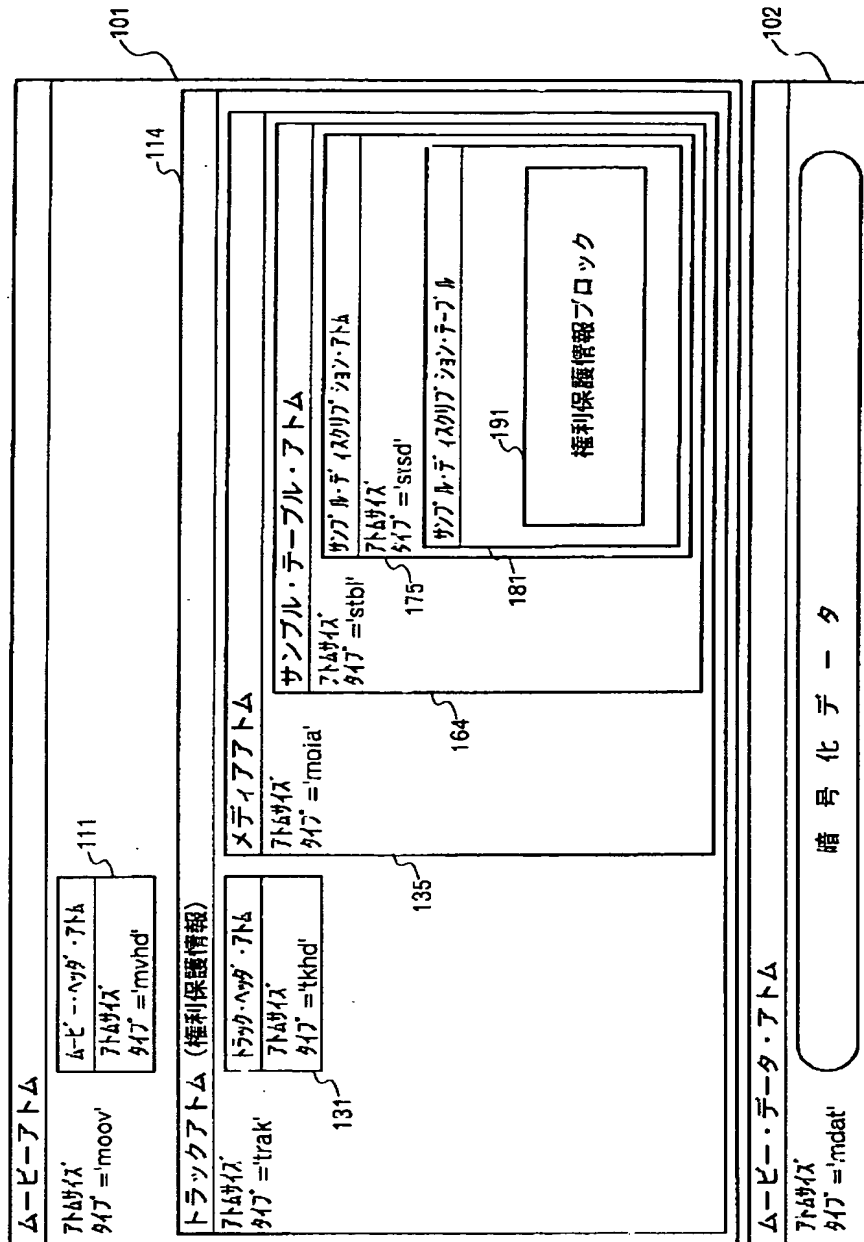
【図3】



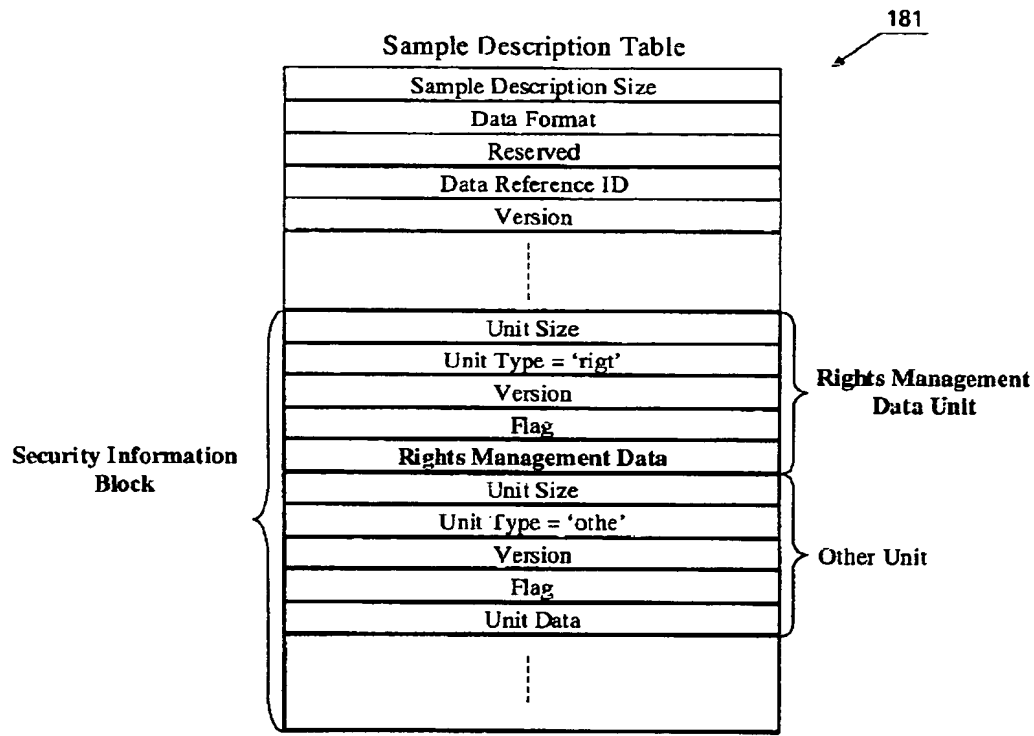
【図2】



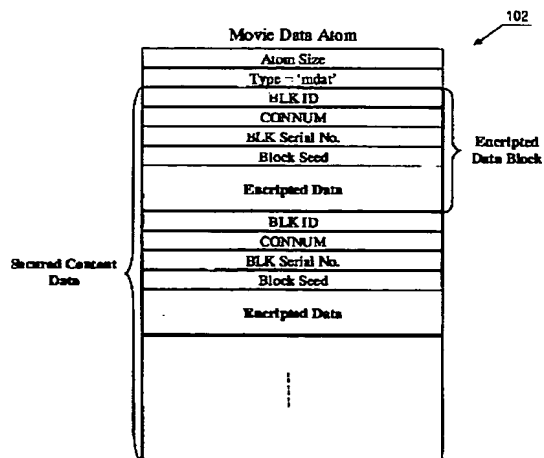
【図4】



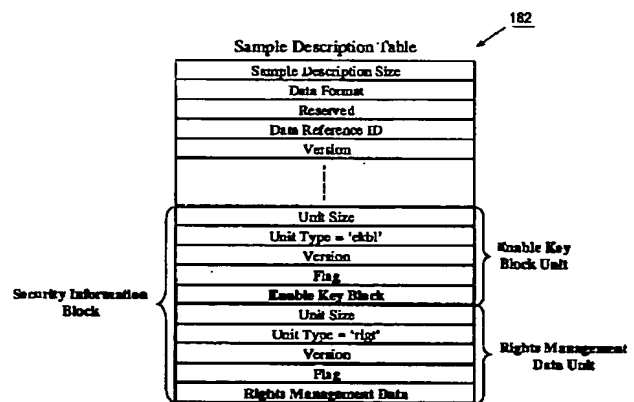
【図5】



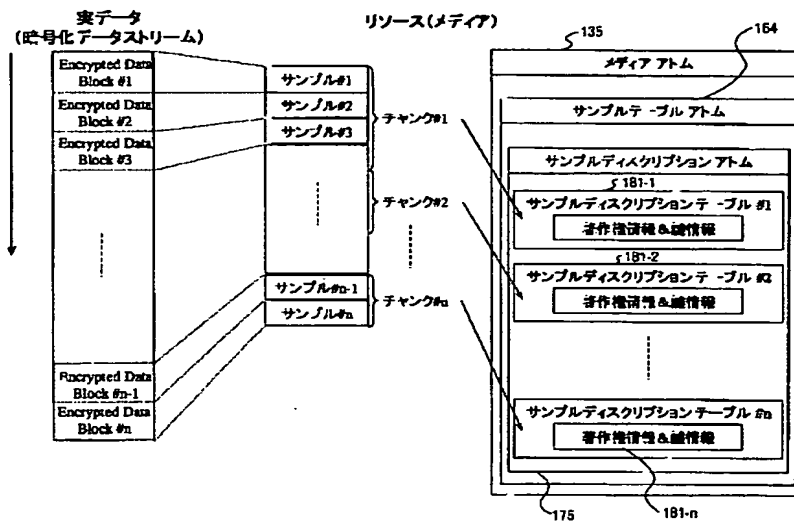
【図7】



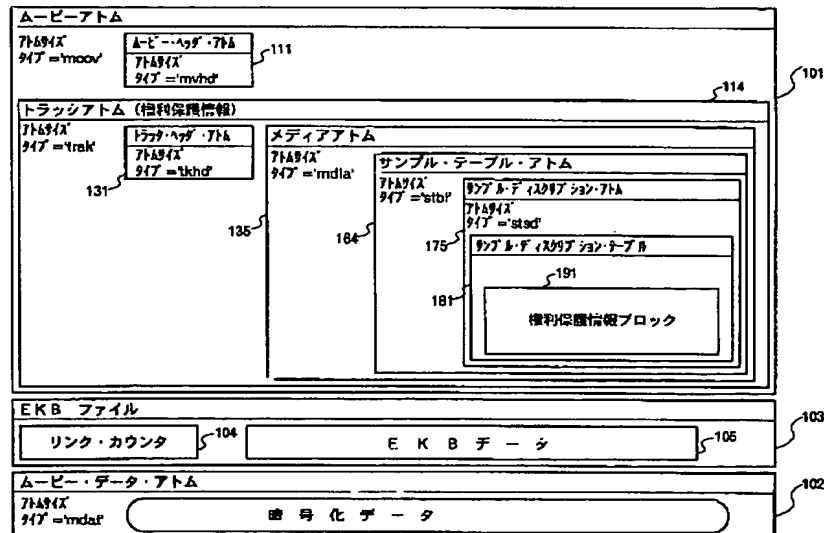
【図9】



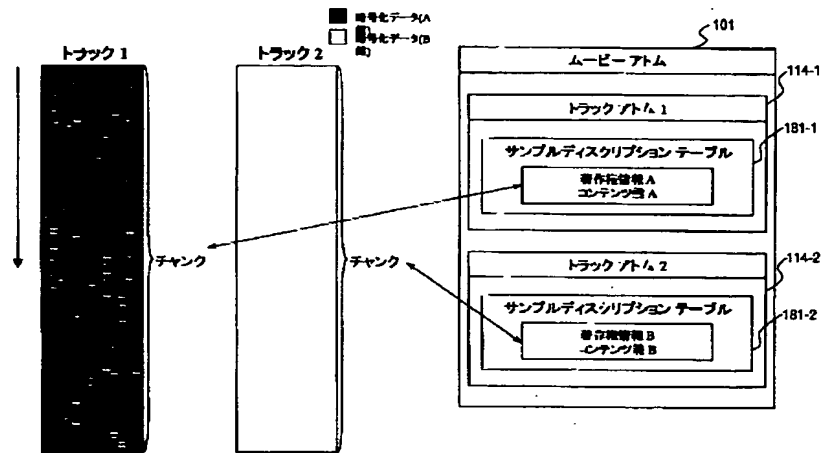
【図8】



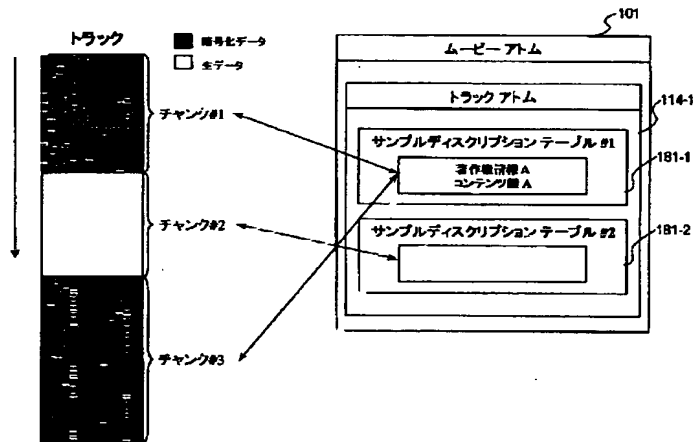
【図11】



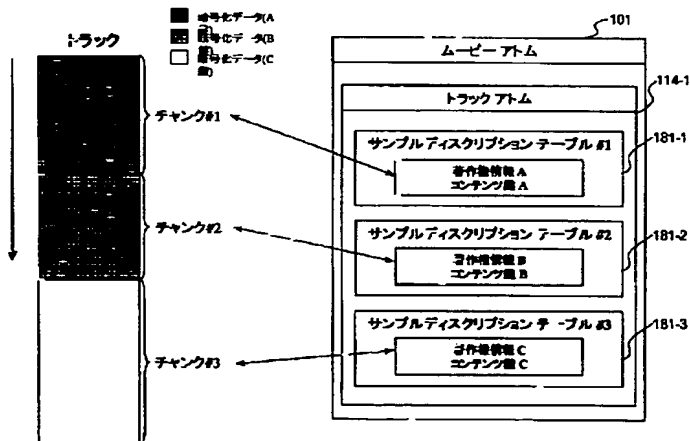
【図13】



【図14】



【図15】



フロントページの続き

(51)Int.Cl. <sup>7</sup>	識別記号	F I	(参考)
G 1 1 B 20/12	1 0 3	G 1 1 B 20/12	1 0 3
27/00		27/00	D
H 0 4 N 5/91		H 0 4 N 5/91	P
5/92		5/92	H

(72)発明者 石黒 隆二  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

F ターム(参考) 5B017 AA03 BA07 CA09 CA16  
5B082 EA07 GA02  
5C053 FA13 FA23 GB06 GB11 GB37  
JA01 JA21 LA11  
5D044 AB05 AB07 BC06 CC04 DE02  
DE49 DE50 DE52 GK17  
5D110 AA17 DA04 DA08 DB02 DE01

This Page Blank (uspto)

This Page Blank (uspto)

This Page Blank (uspto)

This Page Blank (uspto)